



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/009,840

05/01/2002

Olivier Lenoir

USB99 JMC SCU

1234

466 7590 12/16/2005

YOUNG & THOMPSON
745 SOUTH 23RD STREET
2ND FLOOR
ARLINGTON, VA 22202

EXAMINER

BLUDAU, BRANDON S

ART UNIT

PAPER NUMBER

2132

DATE MAILED: 12/16/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 10/009,840	Applicant(s) LENOIR ET AL.	
	Examiner Brandon S. Bludau	Art Unit 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 01 May 2002.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-12 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-12 is/are rejected.
- 7) ☒ Claim(s) 8 and 10 is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date: _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date: _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Claim Objections

1. Claims 8 and 10 are objected to because of the following informalities: in claim 8 the word "key" is omitted in the first line which should read "the step of receiving the encryption key". Claim 10 line 8 there is a misspelling of the word "for". Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claim 4 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Line 4 of claim 4 is confusing and unclear, the examiner assumes the limitation to read "applying a client user known key [that is] embodied within the server authentication database".

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 1-5,7,9-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ratayczak (US Patent 6259909), and further in view of Allahwerdi (US Patent 6928558).

Art Unit: 2132

4. As per claim 1, Ratayczak discloses a process of securing the access to a data processing server from a client site through at least a first communication network, this server comprising means for handling a protocol of authenticating a client site user, comprising a sequence of receiving and processing identification data of a client site user, and a sequence of transmitting a message from the server site to a client site user owned communication equipment through a second communication network (column 6 line 59- column 7 line 23), characterized in that this transmitted message is a voice message (column 7 lines 36-47 wherein using a telephone it is inherent that a voice message is sent) providing to the aforesaid user means for generating an authentication password intended to be transmitted to the aforesaid server site through either the first or the second communication network, the call number of the aforesaid communication equipment being searched from an authentication data base (column 4 lines 12-25 wherein the number call number is inherently stored in the subscriber-related data).

Ratayczak does not disclose wherein the process provides to the user means for generating an authentication password.

Allahwerdi does disclose a process where the data processor provides the user means for generating an authentication password to be sent back to the processor in column 1 lines 54-62).

Allahwerdi is analogous art because it is directed to authenticating a user on a computer system from a mobile device.

It would have been obvious for one of ordinary skill in the art at the time of the invention to modify Ratayczak to include providing the user with a means for generating a password.

Motivation for one to modify Ratayczak as discussed above would have been to enhance the security of the password transmission as implied by Allahwerdi in column 1 line 51-53.

5. As per claim 2, Ratayczak discloses the securing process according to claim 1, characterized in that it comprises steps of:

Requesting identification data (ID, MPC) from the client site through the first communication network (column 6 lines 59-64);

Processing the aforesaid data (ID, MPC) and searching an authentication database for a client user owned mobile communication equipment call number (this is inherent in column 7 lines 1-5 and 36-44 in that the server must know the call number of the mobile device from the HLR described in column 4 lines 12-24);

Calling the aforesaid communication equipment through at least a second communication network (column 7 lines 1-5 and 36-44);

After establishing a communication with the aforesaid mobile communication equipment, generating a random or pseudo random password (MPA) (column 7 lines 36-40);

Sending a voice message comprising the aforesaid random password through the second communication network (column 7 lines 1-5);

Requesting the user provide, from the client site through the first communication network an authentication password (7 lines 13-15) derived from the aforesaid random or pseudo random password; and

Authenticating the aforesaid authentication password (column 7 lines 13-15).

Ratayczak does not disclose wherein the password from the server is randomly generated or that the authentication password is derived from this random password.

Allahwerdi does disclose wherein a server generates a random number and send this to the user to transform into another password to be sent back to the server for authentication in column 1 lines 55-62.

Obviousness and motivation to combine Allahwerdi are mentioned in relation to claim 1, as the combination here is similar.

6. As per claim 3, Ratayczak discloses the process according to claim 2, characterized in that the authentication password matches the server generated random or pseudo random password transmitted through the mobile communication equipment (column 7 lines 1-13).

7. As per claim 4, Allahwerdi discloses in regards to claim 3, a process characterized in that the authentication password is built from the random or pseudo random password generated by the server and transmitted through the mobile communication equipment, applying a client user known and embodied within the server authentication data base key, the authentication step comprising a step of converting the aforesaid authentication password into a random or pseudo random authentication

Art Unit: 2132

password by applying the aforesaid key (column 1 lines 55-62 where one of ordinary skill in the art can see that an encryption key is inherent in the encrypting process).

Allahwerdi is analogous art because it is directed to authenticating a user on a computer system from a mobile device.

It would have been obvious for one of ordinary skill in the art at the time of the invention to modify Ratayczak to include the server submitting a random password for generation into an authentication password based on a key and transmitted to a server to be decrypted.

Motivation for one to modify Ratayczak as discussed above would have been to enhance the security of the password transmission as implied by Allahwerdi in column 1 line 51-53.

8. As per claim 5, Ratayczak discloses the process according to claim 1, characterized in that the identification data requested from the client consists of a couple [identification code/client password] (column 6 lines 59-64).

9. As per claim 7, Ratayczak discloses the securing process according to claim 1, characterized in that it comprises on the server side the steps of:

Requesting identification data (ID, MPC) from the client site through the first communication network (column 6 lines 59-64);

Processing the aforesaid data (ID, MPC) and searching an authentication database for a client user owned mobile communication equipment call number (this is inherent in column 7 lines 1-5 and 36-44 in that the server must know the call number of the mobile device from the HLR described in column 4 lines 12-24);

Calling the aforesaid communication equipment through at least a second communication network (column 7 lines 1-5 and 36-44);

In case the communication is established with the aforesaid mobile communication equipment, send a voice message requesting the user to send an encryption key (Column 4 lines 55-62, wherein the codeword can be used as an encryption key as stated in column 7 lines 59-62)

Receiving and recognizing the encryption key transmitted by the client by means of the mobile equipment keyboard (column 4 lines 59-65),

But does not disclose deciphering by means of the aforesaid encryption key an authentication password transmitted by the client through the first communication network, this password resulting from the encryption of a client password performed at the client site by means of the encryption key; and authenticating the client password which results from the authentication password deciphering

Allahwerdi does disclose deciphering by means of the aforesaid encryption key an authentication password transmitted by the client through the first communication network, this password resulting from the encryption of a client password performed at the client site by means of the encryption key; and authenticating the client password which results from the authentication password deciphering (column 1 lines 55-62).

Allahwerdi is analogous art because it is directed to a method for authenticating a user in a computer system.

It would have been obvious for one of ordinary skill in the art at the time of the invention to modify Ratayczak to include using the requested and sent key at the server to decrypt the previously transmitted password to uncover a subsequent password.

Motivation for one to modify Ratayczak as discussed above would have been to enable the transmission of a password without sending the password unencrypted so as to foil interception as is well known by one of ordinary skill in the art.

10. Claim 9 is rejected because it discloses the same subject matter as claim 1.
11. Claim 10 is rejected because it discloses the same subject matter as claim 2.
12. Claim 11 is rejected because it discloses the same subject matter as claim 7.
13. Claim 12 is rejected in regards to claim 1 because it is directed to an application for utilizing the process of claim 1.
14. Claims 6 and 8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ratayczak (US Patent 6259909), in view of Allahwerdi (US Patent 6928558), and further in view of Fielder (US Patent 5995624)
15. As per claim 6, Ratayczak and Allahwerdi disclose the process according to claim 1, but do not disclose wherein the process is characterized in that the step of requesting the authentication password from the user takes place during a predetermined time-out delay beyond which authentication is denied.

Fielder does disclose wherein the process is characterized in that the step of requesting the authentication password from the user takes place during a predetermined time-out delay beyond which authentication is denied (column 8 lines 45-49).

Art Unit: 2132

Fielder is analogous art because it is directed towards authenticating a user from entry of a password.

It would have been obvious for one of ordinary skill in the art to modify Ratayczak et al. to include a time out interval in which the authentication password needed to be entered.

Motivation for one to modify Ratayczak as discussed above would have been to enhance the security of the process as would be well known by one of ordinary skill in the art.

16. As per claim 8, Ratayczak and Allahwerdi disclose the process according to claim 7, but do not disclose wherein it is characterized in that the step of receiving the encryption [key] takes place during a predetermined time-out delay beyond which the authentication is denied.

Fielder does disclose wherein receiving the encryption [key] takes place during a predetermined time-out delay beyond which the authentication is denied (column 8 lines 45-49).

Obviousness and motivation to combine are the same as presented in claim 6 above as it is a similar limitation.

Conclusion

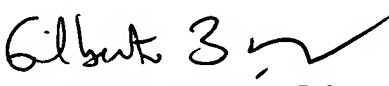
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon S. Bludau whose telephone number is 571-272-3722. The examiner can normally be reached on Monday -Friday 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Brandon S Bludau
Examiner
Art Unit 2132

BB


GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100